Bibliographic data: CN 1178951 (A)

Special grouped filter fire-proof wall

Publication date:	1998-04-15
Inventor(s):	HE WEIDONG [CN] +
Applicant(s):	TIANRONGXIN TECHNOLOGY AND TRA [CN] +
Classification:	**- international:** ***G06F19/00;*** (IPC1-7): G06F19/00 **- European:**
Application number:	CN19971015121 19970723
Priority number(s):	CN19971015121 19970723

Abstract of CN 1178951 (A)

The present invention is used for computer network within enterprise and the fireproof wall consists of four parts including group filter, safety controller, system managing device and card reader. The group filter is located between internet and router; the safety controller is located between system managing device and internet to isolate and protect the system managing device; the card reader is connected to system managing device. When the system managing device configurates control parameter inside fireproof wall relating to network safety, it is necessary to insert safety card into cardreader and to input correct PIN before entering configuration state.

[19]中华人民共和国专利局

[51]Int.Cl[6]
G06F 19/00

[12] 发明专利申请公开说明书

[21] 申请号 97115121.0

[43]公开日 1998 年 4 月 15 日

[11] 公开号 CN 1178951A

[22]申请日 97.7.23

[71]申请人 北京天融信技贸有限责任公司

地址 100080北京市海淀区科学院南路8号

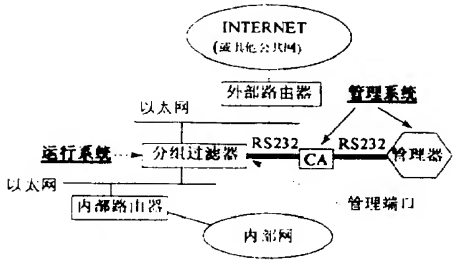
[72]发明人 贺卫东

权利要求书 3 页 说明书 10 页 附图页数 5 页

[54]发明名称 专用分组过滤防火墙

[57]摘要

本发明是一种用于企业内部网的专用分组过滤防火墙，它由分组过滤器、安全控制器、系统管理器和读卡器四部分组成。分组过滤器位于 Intranet 与路由器之间，安全控制器位于系统管理器和 Intranet 之间，对系统管理器进行隔离保护；读卡器与系统管理器相连，系统管理器要对防火墙中涉及网络安全控制参数进行配置时，必须向读卡器口插入安全卡，并输入正确的 PIN，才能进入配置状态。



97.07.23

权　利　要　求　书

1.一种专用分组过滤防火墙，其特征在于，

(1)它由分组过滤器、安全控制器、系统管理器和读卡器四部分组成；

(2)分组过滤器的硬件平台是基于工业级的PC主板(80486以上)或其它类似设备，基本操作系统平台是DOS3.0以上版本，其专用分组过滤软件是基于以上平台的一个DOS应用程序，分组过滤器位于企业内部网与路由器之间；

(3)安全控制器位于系统管理器和企业内部网之间，对系统管理器进行隔离保护，使之免受来自网络的侵扰，另一方面对系统管理器与分组过滤器之间的数据传输采用加密技术，同时对网络内的分组过滤器进行鉴别和认证；

(4)系统管理器经由安全控制器与企业内部网连接，实施对本发明系统设备的设置、监视、运行参数(含访问控制表)的配置和控制；

(5)读卡器与系统管理器相连，当系统管理器要对防火墙中涉及网络安全控制参数进行配置时，必须向读卡器口插入安全卡，并输入正确的个人识别号码才能进入配置状态。

2. 根据权利要求1所述的分组过滤器，其特征在于，

(1)分组过滤器软件功能模块主要由信息获取、规则匹配、缓存维护和分组审计四个部分构成；

(2)信息获取用于获取IP分组中的有关IP的信息，以及TCP头、UDP头或ICMP头中的有关信息，存放到一个数据结构中，供规则匹配时使用；

(3)规则匹配集体完成将指定IP数据报与分组过滤规则集中各规则进行规则匹配的工作，并返回相应的匹配结果；

(4)本分组过滤器的分组过滤原理采用分片缓存和状态缓存的机制；

(5)缓存维护部分执行对分片缓存和状态缓存二者的管理；

(6)分组审计负责对被过滤的IP数据报进行统计和日志。

3.根据权利要求2所述的分组过滤器，其特征在于，

(1)分组过滤器通过DOS的命令解释器运行后，多线程核心调度模块接管整个系统，系统的基本运行单位是线程和中断，采用非抢占的线程调度策略；

(2)内存管理采用基于DOS的内存块链，实现自身的堆空间管理；

(3)文件系统管理采用基于DOS的常规文件系统；

(4)TCP/IP协议栈实现了比较完整的TCP/IP协议族，分组过滤规则可作用于各个网络接口上，由分组过滤模块分别对进入和流出接口的IP分组进行过滤；

(5)分组过滤器对网络接口上输入/输出分组的处理流程是，输入/输出的IP分组都要通过分组过滤模块的检查才能进入IP路由模块，把分组过滤规则加载到某一个接口上以后，分组过滤模块根据过滤规则对进/出该接口的每个IP分组进行检查，作出通过、拒绝通过、审计等操作。

4.根据权利要求1所述的安全控制器，其特征在于

(1)安全控制器由中央控制模块、输入/输出控制模块、安全控制模块、通信控制模块和安全卡鉴别模块等功能模块构成；

(2)安全控制器由一台离线的专用硬件设备和一套相应的专用软件组成，它一方面对系统管理器进行隔离保护，使之免受来自网络的侵扰，另一方面使用加密技术保护系统管理器与分组过滤器之间的数据传输，同时对网络内的分组过滤器进行

鉴别和认证；

(3)安全控制器硬件的内部选件尽可能采用工业级器件，整个机箱为一个防撬、防震设备，机壳无螺钉结构，由安装在机箱后背板左右的两把特制的锁锁定机箱；机箱后背板上除两把锁外有以下接口：一个与安全控制器通讯用的DB9通讯口(Male)，一个与系统管理器通讯用DB9(Male)，一个220伏电源插座；另外，由安装在后背板上的电源开关控制机器的开关；

(4)安全控制器软件是一组建立在DOS软件平台上的应用程序，其功能模块包括：使用安全卡作为系统安全管理人员的资格证书，并向使用人员分发随机若干位数字的个人身份识别号码等；

(5)安全卡中存放两种内部信息，一是用于在系统管理器对防火墙涉及网络安全配置(含访问控制表)的重置、修改、增/删等操作进行授权认证；二是对分布在企业内部网络内各个子网上的防火墙的合法性认定；内置加密卡(或驻留加密软件)，为系统管理器对各个子网上防火墙的配置以及其他涉及网络安全的信息传输进行数据加密/解密；设计与系统管理器、读卡器和以太网之间的通信模块；设计来自系统管理器的命令识别模块；设计对系统管理器、防火墙的合法性资格认定模块。

5.根据权利要求1所述的系统管理器，其特征在于，

(1)它由一台486以上微机或专用机和一套专用管理软件包组成，该软件包是建立在MS-DOS 6.0以上版本、Microsoft Windows 3.1以上版本以及Hp OpenView for Windows C-02-06以上版本的软件平台上的应用软件，利用Hp OpenView for Windows中嵌入的SNMP进行防火墙系统的设备配置；

(2)专用管理软件包采用的技术手段有：利用OpenView for Windows中的网络映射和子网映射模块构造本系统的设备参数配置模块；根据防火墙设计规范中关于防火墙配置文件(含访问控制表)格式，设计文本编辑器和配置文件编译器模块；设置防火墙运行必要参数的设置、修改、增/删格式模块；设计防火墙之间进行安全通信的参数配置模块；利用从安全控制器和过滤器中传送来的审计信息、统计信息和陷阱信息进行分类处理的功能模块。

(3)本系统管理器执行的过滤器参数配置的基本内容有网络接口的IP地址、IP路由表、网络接口上的分组过滤规则集、分组过滤规则集内的规则等，系统管理则采用了分布式的体系结构即客户机/服务器模式。

6.根据权利要求1所述的专用分组过滤防火墙，其特征在于，

(1)分组过滤器代理驻留在被管对象分组过滤器上，通过FCMP接收系统管理器发来的配置命令，由命令解释器/规则编译器执行后将配置参数注入分组过滤器中，从而控制本发明系统的运行，分组过滤器代理与系统管理器之间的通信方式为客户机/服务器模式；

(2)FCMP协议定义了分组过滤器、系统管理器之间的请求(管理器)-应答(过滤器代理)对的格式及同步关系，当过滤器代理监测到系统中发生的一些“敏感”事件时，也可利用FCMP TRAP主动发起请求，通知系统管理器；

(3)通过系统管理器的用户界面来定义对分组过滤器的配置要求，系统管理器把这些配置要求通过FCMP告诉过滤器代理，并最终决定分组过滤器的参数和状态。

7.根据权利要求1所述的专用分组过滤防火墙，其特征在于，分组过滤器、安全控制器和系统管理器之间的数据传输采用了加密传输技术。

8.根据权利要求1所述的专用分组过滤防火墙，其特征在于，安全控制器代理包括

代理过滤器和代理管理器两部分，代理过滤器接收来自管理器的请求，交代理管理器传给过滤器，代理管理器接收来自过滤器的请求，交代理过滤器传给管理器。

97.07.23

说　　明　　书

专用分组过滤防火墙

本发明涉及一种用于企事业单位内部计算机网络(企业内部网)的专用分组过滤防火墙，它属于计算机网络安全防火墙(firewall)技术。

目前中国尚无自己的专用分组过滤防火墙，国外的分组过滤功能往往出现在路由器中，比如Cisco公司的Cisco 2501路由器，其缺点是：路由器上的分组过滤是路由器的附加功能，过滤细度不够，各种安全要求不可能充分满足；过滤规则的数目有限，且随着规则数目的增加，路由器性能会受到影响；缺少必要的报警、审计机制；另外，由于路由器的高度专业化，在路由器的分组过滤器上定义和维护规则集也比较困难。目前分组过滤规则集的复杂化已是一个发展趋势，规则复杂化表现为增加更多的域(比如时间)，规则之间也开始发生关系，不再是静态地各自为阵。分组过滤器本身的发展则要求对其分组流状态进行跟踪记录，以处理动态的分组流，而不仅仅是处理静态的一个一个的分组。这首先要求平台应有更强大的处理能力，其次过滤器应当从分组中提取出更多有用的信息。更重要的是，我国的网络信息安全不能建立在国外的信息安全产品上。

本发明的目的在于：提供一种设置于公共计算机网络与企业内部网之间、可升级、不影响路由器正常路由功能、有审计报警功能、平台处理能力强、具有自主版权和自身安全保护手段的专用分组过滤防火墙。

本发明的任务是以下述方式实现的：

本发明由分组过滤器、安全控制器、系统管理器和读卡器四部分组成。系统管理器(简称管理器)经由安全控制器与企业内部网连接，实施对本发明系统设备的设置、监视、运行参数(含访问控制表)的配置和控制；安全控制器位于系统管理器和企业内部网之间，一方面对系统管理器进行隔离保护，使之免受来自网络的侵扰，另一方面使用加密技术保护系统管理器与分组过器之间的数据传输，同时对网络内的分组过滤器进行鉴别和认证；分组过滤器(简称过滤器)位于企业内(总部及其分支机构)各个专用网络与路由器之间，支持企业内部各个子网络(专用网络)之间在TCP/IP环境下的信息“通过/阻断”安全运行方式；读卡器与系统管理器相连，当系统管理器要对防火墙中涉及网络安全控制参数进行配置时，必须向读卡器口插入安全卡，并输入正确的个人识别号码(PIN)，才能进入配置状态。

系统管理器与安全控制器硬件采用RS232串行接口连接，相应的通信软件可保证系统管理器在授权认证后对防火墙、企业内部网用户以及网际探测操作的透明性和完整性。

安全控制器一方面利用串口分别与系统管理器、读卡器相连，另一方面利用网卡与LAN的以太电缆和集线器相连，其通信软件应保证与相关设备(含跨地域公共网的防火墙)通信的透明性和完整性。

分组过滤器的内侧端(Private port)采用AUI标准与企业内部专用网的以太电缆和集线器相连，外侧端(Public port)采用AUI标准与路由器的AUI口相连，如果企事业单位网络设置有网关和堡垒机等，那么防火墙的外侧端则与相应的以太电缆或集线器连接。与之相应的通信软件应确保对所有进/出数据的传输是透明的、完整的。

系统管理器、安全控制器和分组过滤器构成完整的本发明系统。各子系统一方面有

自己的系统自举程序和常规操作软件，另一方面各子系统之间不但有信息交换和相互识别认证的功能，而且系统管理器对网络部件的配置参数和映射数据与安全管理器、分组过滤器的相关配置参数保持一致。从而保证本发明各子系统软件功能的相互协调性。

本发明从功能上可简单地分为运行系统和管理系统两部分。运行系统指分组过滤器，它完成对IP分组的过滤以保证内部网络的安全；管理系统包括安全管理器、系统管理器和读卡器，以及分组过滤器的一部分，其作用是对分组过滤器进行配置和监控，并提供安全手段以保证本发明整个系统的安全。

本发明的主要功能包括：1.防止公共网上某些不被企业安全政策许可的信息和服务进入内部网；2.防范未经授权的用户从公共网上攻击并侵入防火墙系统本身或企业内部网，恶意破坏或滥用其中的资源；3.为公共网上许可的用户(主机或网络)提供企业安全策略许可的内部信息和服务的访问通道，为企业内部用户访问公共网上的企业安全策略许可的公共信息和服务提供访问通道；4.监视流经防火墙的信息流，登记发生的侵犯和违规事件；5.提供对防火墙的监控和配置管理；6.提供对防火墙的安全管理；7.监控对防火墙的所有操作等。

以上第1、2、3项功能是本发明的外部功能，第4、5、7项是本发明的内部功能，第6项是本发明的内部安全性所在。

本发明的外部安全功能由分组过滤器实现，它的监控和配置管理通过一台离线的PC机加上相应的软件实现。第4项是分组过滤器的内部软件功能，第7项是安全控制器的内部软件功能。分组过滤器通过对IP分组的过滤以保证内部网络的安全。

分组过滤器的硬件平台是基于工业级的PC主板(80486以上，本发明的实现方式为80586系统，具有640K常规内存和360K扩展内存，以及100M以上的硬盘空间)或其它具类似功能的设备，基本操作系统平台是DOS(版本3.0以上)。其专用分组过滤软件是基于以上平台的一个DOS应用程序。

本分组过滤器为专用硬件设备，它是需要24小时不间断运行的安全设备，故整体结构采用防震、防撬，内部选件尽可能采用工业级器件。整个机箱为一个防撬、防震设备，机壳无螺钉结构，由安装在机箱后背板左右的两把特制的锁锁定机箱。机箱内装有PS250工业电源、PCM5860工控板、2.5寸硬盘(210M)、Intel PCI网卡(NE2000兼容网卡)、Intel Pentium 150CPU，Pentium CPU冷却风扇、4M内存和专用通信电缆。

分组过滤器的机箱后背上除两把锁外有以下接口：一个与安全控制器通信用的DB9通信口(Male)，一个与路由器相连的网络通信口(RJ45)及其状态显示灯(绿色)，一个与内部局域网相连的网络通信口(RJ45)及其状态显示灯(绿色)，一个220V电源插座。另外，由安装在后背板上的电源开关控制机器的开关。

分组过滤器的主要功能有：分组过滤功能，确保企业内部网在TCP/IP环境下的资源保护；记录通信事件，统计数据业务量(Traffic)情况并供系统管理器检索；审计违规事件并做详细记录，定期传送给系统管理器；加密传送(根据配置需要)等。

分组过滤模块完成对指定IP分组的分组过滤工作，并对所有接受过滤的分组进行统计和作相应的日志。分组过滤模块主要由信息获取、规则匹配、缓存维护和分组审计四个部分构成。信息获取用于获取IP分组中的有关IP的信息，以及TCP头、UDP头或ICMP头中的有关信息，存放到一个数据结构中，供规则匹配时使用。规则匹配集体完成将指定IP数据报与分组过滤规则集中各规则进行规则匹配的工作，并返回相应的匹配结果。在分组过滤的时候，为了提高过滤的效率，采用了分片缓存和状态缓存的机制。缓存维护部分便是用于对二者的管理，如缓存的检测、增加、删除等。分组审计负责对被过滤的IP数据报进行统计和日志。

分组过滤模块的内部结构及其与外部模块间的逻辑关系如附图4所示。

本分组过滤器根据Cisco路由器的分组过滤方法，开发出系统配置、访问控制表以及企业用户常用的网络服务配置的规则及格式。其基于TCP/IP的访问控制表，能对IP地址、传输协议、服务类型、服务端口号进行配置(必要时可进行灵活组配)并准确实施之，访问控制表的实施软件可准确地探测外部IP地址的欺骗行为。分组过滤器之间定期交换基本运行状态数据，确保内部网络各信道畅通。分组过滤器可内置加密卡(或内驻加密软件)，为系统管理器对分组过滤器的参数配置以及涉及网络安全的信息传输进行数据加密，同时为企业内部用户间的业务通信数据提供加密传输，以形成跨地域公共网络的内部网络的内部安全信道。本分组过滤器还根据企事业单位网络的使用特点，可对加密传输、密钥更换、业务往来及审计信息等加配时间域(或时间陷阱)。本分组过滤器可对违规事件(暂时定义为凡在配置文件中找不到匹配条件的访问，以及分组过滤器不认识的通信事件)按时间、源地址(IP地址或MAC地址)、目的地址(IP地址或MAC地址)、行为(希望请求的通信、服务及其它)等详细记录在机内缓存区，定时传送给系统管理器或供系统管理器检索。

分组过滤器通过DOS的命令解释器运行后，多线程核心调度模块接管整个系统。这时，系统的基本运行单位是线程和中断。为了简化系统设计和避免DOS重入问题，采用非抢占的线程调度策略。内存管理基于DOS的内存块链，实现自身的堆空间管理以最大限度地利用系统内存和克服单任务系统的栈堆检查。文件系统管理也是基于DOS的常规文件系统。需要注意的是，多线程调度及其相应的内存管理策略对处理网络环境下的许多并发事件是必需的。

TCP/IP协议栈实现了比较完整的TCP/IP协议族。分组过滤规则可作用于各个网络接口上，由分组过滤模块分别对进入和流出接口的IP分组进行过滤。分组过滤器对网络接口上输入/输出分组的处理流程见附图3。系统中输入/输出的IP分组都要通过分组过滤模块的检查才能进入IP路由模块。把分组过滤规则加载到某一个接口上以后，分组过滤模块就根据规则对进/出该接口的每个IP分组进行检查，作出通过、拒绝通过、审计等操作。

本分组过滤器的过滤根据和标准是基于以下内容：分组源地址和子网模(支持域名和IP地址)；分组宿地址和子网模；分组源端口(仅对TCP/UDP协议)；分组宿端口(仅支持TCP/UDP协议)；传输协议，包括TCP，UDP，ICMP，UGP等协议；与分组相关的网络接口；分组的IP选项(可选)支持19个IP选项和8个安全选项；分组的TOS(服务类型)；分组的平均生存时间(TTL)；已分片的分组(包括过短的分组)，分片的分组在IP分组过滤欺骗中起了很大作用；TCP头(对于TCP协议)中的标志，共6个标记；ICMP类型/代码(对于ICMP协议)常用，共11种类型域，每种类型域又分若干代码；日期和时间(可选)，可以在日期和时间上控制网络的流量和类型；用户数据(可选)，针对于特定的协议。

分组过滤器的统计分组量包括被阻塞的分组数、没有找到匹配的分组数、通过的分组数、被log的分组数和分组的总量等等。

本发明管理系统包括系统管理器、安全控制器、读卡器、过滤器代理和它们之间用来交换管理信息的防火墙控制信息协议(FCMP协议)。

安全控制器由中央控制模块、输入/输出控制模块、安全控制模块、通信控制模块和安全卡鉴别模块等构成。安全控制器由一台离线的专用硬件设备和一套相应的专用软件组成，它一方面对系统管理器进行隔离保护，使之免受来自网络的侵扰，另一方面使用加密技术保护系统管理器与分组过滤器之间的数据传输，同时还可对网络内的防火墙进行鉴别和认证。

安全控制器的主要功能包括：隔离网络对系统管理器的访问；使用加密技术保护系统管理器和网络上防火墙之间的数据传送；对系统管理器与防火墙的重要通信进行授权

认证；对企业内部网上的所有防火墙进行合法性认定；对系统管理器来的重要事件以及安全管理器本身操作的重大事件进行记录、存储并定期传送给系统管理器。

安全控制器硬件为一专用设备，它需要24小时不间断运行并且保证安全，故内部选件尽可能采用工业级器件，整个机箱为一个防撬、防震设备，机壳无螺钉结构，由安装在机箱后背板左右的两把特制的锁锁定机箱。机箱后背板上除两把锁外有以下接口：一个与安全控制器通讯用的DB9通讯口(Male)，一个与系统管理器通讯用DB9(Male)，一个220伏电源插座。另外，由安装在后背板上的电源开关控制机器的开关。

安全控制器机箱内的装置有PS250工业电源、PCM4862工控板、2.5寸硬盘(210M)、AMD486DX4/100、486CPU冷却风扇、4M内存和专用通信电缆等。

安全控制器软件是一组建立在DOS软件平台上的应用程序，其功能包括：使用安全卡(安全卡是一种IC卡或智能卡)作为系统安全管理人员的资格证书，并向使用人员分发随机若干位数字的个人身份识别号码(PIN)；安全卡中存放两种内部信息，一是用于在系统管理器对防火墙涉及网络安全配置(含访问控制表)的重置、修改、增/删等操作进行授权认证；二是对分布在企事业单位网络内各个子网上的防火墙的合法性认定；内置加密卡(或驻留加密软件)，为系统管理器对各个子网上防火墙的配置以及其他涉及网络安全的信息传输进行数据加密/解密；设计与系统管理器、读卡器和以太网之间的通信模块；设计来自系统管理器的命令识别模块；设计对系统管理器、防火墙的合法性资格认定模块。

系统管理器由一台486以上微机或专用机和一套专用管理软件包组成。该软件包是建立在MS-DOS 6.0以上版本、Microsoft Windows 3.1以上版本以及Hp OpenView for Windows C-02-06以上版本的软件平台上的应用软件。利用Hp OpenView for Windows中嵌入的SNMP进行防火墙系统的设备配置，网络管理极为方便。

其主要技术手段有：利用OpenView for Windows中的网络映射和子网映射模块构造本系统的设备参数配置模块；根据防火墙设计规范中关于防火墙配置文件(含访问控制表)格式，设计文本编辑器和配置文件编译器模块；设置防火墙运行必要参数的设置、修改、增/删格式模块；设计防火墙之间进行安全通信的参数配置模块；利用从安全控制器和过滤器中传送来的审计信息、统计信息和陷阱信息进行分类处理的功能模块；使用合适的语言设计GUI人机界面。

系统管理器的主要功能包括：定义系统组件(安全控制器和分组过滤器)的设备参数，使之作为一个整体协调工作；定义防火墙运行所必须维持、修改、增/删的网络参数(本地子网参数、防火墙之间的信息交换参数、网关或堡垒机参数、远程子网参数、路由器参数、对防火墙的审计参数等)；制定网络访问控制表，经编辑-编译后驻留于防火墙内作过滤控制规则；定义防火墙之间进行安全通信的参数(防火墙标识、IP地址、加密的时间单位、时间长度、数据流动方向、是否记录等)；监视和审计，转储安全控制器和分组过滤器的数据流动信息、配置信息和审计信息，进行分类、统计、显示/打印。

读卡器可为任一种商用读卡器，本发明采用的是Bull CP8读卡器，读卡器使用专用的变压器外接220V电源，通过其专用的通信电缆(DB9-RJ45)与系统管理器的计算机进行通信。读卡器可直接安放在操作台上。

本发明管理系统的主要功能是对过滤器的各项参数作出配置和对过滤器的运行情况进行监视；并且，为了保证过滤器的安全，要对过滤器管理人员的身份进行鉴别，还要对管理系统和运行系统间的通信进行加密传输。

过滤器参数配置的基本内容包括网络接口的IP地址、IP路由表、网络接口上的分组过滤规则集、分组过滤规则集内的规则等。为了便于通过网络对过滤器进行集中的管

理，本管理系统采用了分布式的体系结构(即客户机/服务器模式)。　过滤器代理驻留在被管对象分组过滤器上，通过FCMP接收管理器发来的配置命令，由命令解释器/规则编译器执行后将配置参数注入运行系统中，从而控制系统的运行。总的来说，过滤器代理与管理器之间的通信方式为客户机/服务器模式。FCMP协议定义了二者之间的请求(管理器)-应答(过滤器代理)对的格式及同步关系。当过滤器代理监测到系统中发生的一些“敏感”事件时，也会利用FCMP TRAP主动发起请求，通知管理器。

系统管理员通过系统管理器的用户界面来定义对分组过滤器的配置要求，管理器把这些配置要求通过FCMP告诉过滤器代理并最终影响运行系统的参数和状态。

SDLP(简单数据链路协议)协议是一个特地为点对点直连线路(RS-232C)设计的数据链路层协议。由于认定管理器与安全控制器之间、安全控制器与过滤器之间的RS-232C物理线路是可靠的，SDLP收发的功能不象其他数据链路层协议如HDLC、LAPB、LCP一样还提供流量控制、差错恢复、链路维护等功能。

SDLP的设计目标是：(1)为上层协议(如FCMP)提供一种无确认、无连接服务，丢失帧和差错帧的恢复由上层完成；(2)进行链咯帧的识别与封装，SDLP的下层驱动程序提供带缓冲的有序字节流传输服务，SDLP要将下层来的字节流组合成帧，并将上层的数据封装成帧后分解成有序字节流发送出去；(3)检测传输差错，丢失差错帧；(4)为上层提供设计良好的链路层服务接口。

本发明除了完成分组过滤的功能外，还必须考虑整个系统本身的安全，即保证过滤器只能被合法的管理器管理，且管理信息在传送过程中不被非法获取。本发明本身的安全性是通过安全控制器以及管理信息加密传输实现的。

安全控制器代理包括两部分，一是代理过滤器，二是代理管理器。代理过滤器接收来自管理器的请求，交代理管理器传给过滤器。代理管理器接收来自过滤器的请求，交代理过滤器传给管理器。

分组过滤器软件模块及数据流。过滤器内部运行两大数据流，一是通过RS-232C串行接口、来往于分组过滤器与管理器之间的FCMP请求/应答流(简称FCMP流)，一是进出分组过滤器网络端口的IP分组流。

参与FCMP流的模块有串行端口驱动程序、SDLP模块、加解密模块、FCMP模块、过滤器代理和命令解释模块。过滤器代理是整个FCMP流的中心。它作为一个后台进程(或线索)驻留在系统中，等待来自管理器的FCMP请求，将FCMP请求转换成命令，传给命令解释器；过滤器代理得到命令解释器的执行结果后，将FCMP应答传回管理器。

加解密模块位于FCMP模块和SDLP模块之间，换言之，经SDLP模块和串行端口驱动程序传送的数据都经过加密，而FCMP模块处理的数据均未经加密或已经解密。

过滤器交给命令解释器的命令包括执行命令、配置命令和过滤规则。命令解释器将过滤规则交给过滤规则编译器，编译后放入Startup区的规则表中，供分组过滤模块使用。对于配置命令，命令解释器先进行处理，调用相应函数修改分组过滤器的系统状态，然后将配置命令写入Startup区的系统配置中。对于执行命令，命令解释器调用相应函数处理。

参与IP分组流的模块包括网络端口驱动模块、IP模块和分组过滤模块。分组过滤模块嵌入IP模块中，除对出入IP分组进行过滤外，还负责对过滤过程进行记录。

除上述数据流外，分组过滤器还主动向管理器发送TRAP信息，报告系统初始化、文件系统故障、非法用户侵入等异常情况。TRAP信息的收集和处理由系统监视模块负责。

另外，整个系统的运作都是基于一个操作系统核心进行的。该操作系统核心包括多任务调度核心、内存管理模块、文件管理模块、I/O管理模块。

安全控制器(CA)软件模块及数据流。安全控制器中运行两个FCMP流，一个是代理过滤器与管理器之间的FCMP流，另一个是代理管理器之间的FCMP流。

CA中的两个FCMP流处理过程与分组过滤器中的FCMP流处理过程大致相同。其中代理管理器是FCMP请求的发起者，而代理过滤器是FCMP请求的接收者。代理管理器与分组过滤器构成客户机/服务器，管理器与代理过滤器构成另一对客户机/服务器。代理管理器与代理过滤器之间的信息交换通过一个全局变量区实现。

CA的另一个重要功能是验证管理员的身份，以允许或拒绝对分组过滤器的访问。图中的认证模块实现上是一个身份证算法，建立在SDLP帧的基础上。CA对数据加密时所用到的加密密钥来自一个存放密钥的内部表。

系统管理器的软件模块与数据流。FCMP协议堆栈(含FCMP模块、SDLP模块、串行端口驱动模块)和用户界面是管理器的主要组成部分。其中FCMP协议各模块作为客户端向分组过滤器发送管理员命令，并接收来自分组过滤器的返回结果。由于CA的存在，事实上管理器并不直接跟分组过滤器通信，与管理器通过RS-232C端口直接通信的是CA。管理器FCMP客户的服务器端是CA上的代理过滤器。

管理器的另一重要功能是验证管理人员的身份。合法的管理人员拥有一个表明其身份的IC卡，其中存有管理员的个人识别号码(PIN)。在管理员被允许进入管理器正常操作以前，必须将IC卡插入管理器读卡器中，经IC卡处理模块读入其PIN，然后传到CA上的认证模块进行身份认证。若认证成功，则可进入管理器操作，否则管理器拒绝进入正常操作。

本发明的基本特征是：

(1)它由分组过滤器、安全控制器、系统管理器和读卡器四部分组成；

(2)分组过滤器的硬件平台是基于工业级的PC主板(80486以上)或其它类似设备，基本操作系统平台是DOS3.0以上版本，其专用分组过滤软件是基于以上平台的一个DOS应用程序，分组过滤器位于企业内部网与路由器之间；

(3)安全控制器位于系统管理器和企业内部网之间，对系统管理器进行隔离保护，使之免受来自网络的侵扰，另一方面对系统管理器与分组过滤器之间的数据传输采用加密技术，同时对网络内的分组过滤器进行鉴别和认证；

(4)系统管理器经由安全控制器与企业内部网连接，实施对本发明系统设备的设置、监视、运行参数(含访问控制表)的配置和控制；

(5)读卡器与系统管理器相连，当系统管理器要对防火墙中涉及网络安全控制参数进行配置时，必须向读卡器口插入安全卡，并输入正确的个人识别号码才能进入配置状态；

(6)安全卡中存贮有两种内部信息，一是用于在系统管理器对防火墙涉及网络安全配置(含访问控制表)的重置、修改、增/删等操作进行授权认证；二是对分布在企事业单位网络内各个子网上的防火墙的合法性认定。

分组过滤模块(过滤器软件部分)完成对指定IP分组的分组过滤工作，并对所有接受过滤的分组进行统计和作相应的日志。分组过滤模块主要由信息获取、规则匹配、缓存维护和分组审计四个部分构成。信息获取用于获取IP分组中的有关IP的信息，以及TCP头、UDP头或ICMP头中的有关信息，存放到一个数据结构中，供规则匹配时使用。规则匹配集体完成将指定IP数据报与分组过滤规则集中各规则进行规则匹配的工作，并返回相应的匹配结果。在分组过滤的时候，为了提高过滤的效率，采用了分片缓存和状态缓存的机制。缓存维护部分便是用于对二者的管理，如缓存的检测、增加、删除等。分组审计负责对被过滤的IP数据报进行统计和日志。

分组过滤器通过DOS的命令解释器运行后，多线程核心调度模块接管整个系统。这时，系统的基本运行单位是线程和中断。为了简化系统设计和避免DOS重入问题，采用非抢占的线程调度策略。内存管理基于DOS的内存块链，实现自身的堆空间管理以最大限度地利用系统内存和克服单任务系统的栈堆检查。文件系统管理也是基于DOS的常规文件系统。需要注意的是，多线程调度及其相应的内存管理策略对处理网络环境下的许多并发事件是必须的。

TCP/IP协议栈实现了比较完整的TCP/IP协议族。分组过滤规则可作用于各个网络接口上，由分组过滤模块分别对进入和流出接口的IP分组进行过滤。系统中输入/输出的IP分组都要通过分组过滤模块的检查才能进入IP路由模块。把分组过滤规则加载到某一个接口上以后，分组过滤模块就根据规则对进/出该接口的每个IP分组进行检查，作出通过、拒绝通过、审计等操作。

安全控制器由中央控制模块、输入/输出控制模块、安全控制模块、通信控制模块和安全卡鉴别模块等功能模块构成；它实际上由一台离线的专用硬件设备和一套相应的专用软件组成，它一方面对系统管理器进行隔离保护，使之免受来自网络的侵扰，另一方面使用加密技术保护系统管理器与分组过滤器之间的数据传输，同时对网络内的分组过滤器进行鉴别和认证。

安全控制器硬件为一专用设备，其内部选件尽可能采用工业级器件，整个机箱为一个防撬、防震设备，机壳无螺钉结构，由安装在机箱后背板左右的两把特制的锁锁定机箱。机箱后背板上除两把锁外有以下接口：一个与安全控制器通讯用的DB9通讯口(Male)，一个与系统管理器通讯用DB9(Male)，一个220伏电源插座。另外，由安装在后背板上的电源开关控制机器的开关；

安全控制器软件是一组建立在DOS软件平台上的应用程序，其功能包括：使用安全卡(安全卡是一种IC卡或智能卡)作为系统安全管理人员的资格证书，并向使用人员分发随机若干位数字的个人身份识别号码(PIN)；安全卡中存放两种内部信息，一是用于在系统管理器对防火墙涉及网络安全配置(含访问控制表)的重置、修改、增/删等操作进行授权认证；二是对分布在企事业单位网络内各个子网上的防火墙的合法性认定；内置加密卡(或驻留加密软件)，为系统管理器对各个子网上防火墙的配置以及其他涉及网络安全的信息传输进行数据加密/解密；设计与系统管理器、读卡器和以太网之间的通信模块；设计来自系统管理器的命令识别模块；设计对系统管理器、防火墙的合法性资格认定模块等。

系统管理器由一台486以上微机或专用机和一套专用管理软件包组成。该软件包是建立在MS-DOS 6.0以上版本、Microsoft Windows 3.1以上版本以及Hp OpenView for Windows C-02-06以上版本的软件平台上的应用软件。利用Hp OpenView for Windows中嵌入的SNMP进行防火墙系统的设备配置，网络管理极为方便。其主要技术手段有：利用OpenView for Windows中的网络映射和子网映射模块构造本系统的设备参数配置模块；根据防火墙设计规范中关于防火墙配置文件(含访问控制表)格式，设计文本编辑器和配置文件编译器模块；设置防火墙运行必要参数的设置、修改、增/删格式模块；设计防火墙之间进行安全通信的参数配置模块；利用从安全控制器和过滤器中传送来的审计信息、统计信息和陷阱信息进行分类处理的功能模块；使用合适的语言设计GUI人机界面。

系统管理器与安全控制器硬件采用RS232串行接口连接，相应的通信软件可保证系统管理器在授权认证后对防火墙、企业内部网用户以及网际探测操作的透明性和完整性。

安全控制器一方面利用串口分别与系统管理器、读卡器相连，另一方面利用网卡与

LAN的以太电缆和集线器相连，其通信软件应保证与相关设备(含跨地域公共网的防火墙)通信的透明性和完整性。

分组过滤器的内侧端(Private port)采用AUI标准与企业内部专用网的以太电缆和集线器相连，外侧端(Public port)采用AUI标准与路由器的AUI口相连，如果企事业单位网络设置有网关和堡垒机等，那么防火墙的外侧端则与相应的以太电缆或集线器连接。与之相应的通信软件应确保对所有进/出数据的传输是透明的、完整的。

系统管理器、安全控制器和分组过滤器构成完整的本发明系统。各子系统一方面有自己的系统自举程序和常规操作软件，另一方面各子系统之间不但有信息交换和相互识别认证的问题，而且系统管理器对网络部件的配置参数和映射数据必须与安全管理器、分组过滤器的相关配置参数保持一致。从而保证本发明各子系统软件功能的相互协调性。

本发明管理系统的主要功能是对过滤器的各项参数作出配置和对过滤器的运行情况进行监视；而且，为了保证过滤器的安全，要对过滤器管理人员的身份进行鉴别，还要对管理系统和运行系统间的通信进行加密传输。

过滤器参数配置的基本内容包括网络接口的IP地址、IP路由表、网络接口上的分组过滤规则集、分组过滤规则集内的规则等。为了便于通过网络对过滤器进行集中的管理，本管理系统采用了分布式的体系结构(即客户机/服务器模式)。 过滤器代理驻留在被管对象分组过滤器上，通过FCMP接收管理器发来的配置命令，由命令解释器/规则编译器执行后将配置参数注入运行系统中，从而控制系统的运行。总的来说，过滤器代理与管理器之间的通信方式为客户机/服务器模式。FCMP协议定义了二者之间的请求(管理器)-应答(过滤器代理)对的格式及同步关系。当过滤器代理监测到系统中发生的一些“敏感”事件时，也会利用FCMP TRAP主动发起请求，通知管理器。

系统管理员通过系统管理器的用户界面来定义对分组过滤器的配置要求，管理器把这些配置要求通过FCMP告诉过滤器代理并最终影响运行系统的参数和状态。

本发明除了完成分组过滤的功能外，还必须考虑整个系统本身的安全，即保证过滤器只能被合法的管理器管理，且管理信息在传送过程中不被非法获取。本发明的安全性是通过安全控制器以及管理信息的加密传输实现的。

安全控制器代理包括两部分，一是代理过滤器，二是代理管理器。代理过滤器接收来自管理器的请求，交代理管理器传给过滤器。代理管理器接收来自过滤器的请求，交代理过滤器传给管理器。

下面结合附图对本发明做进一步的说明。

图1是本发明的体系结构图。本发明配置在公共信息网与企业内部网之间，其分组过滤器一端接外部路由器，另一端接内部路由器或内部网络。分组过滤器与安全控制器(CA)、安全控制器(CA)与系统管理器之间的连接采用RS232接口。

图2是本发明过滤器结构框图。分组过滤器的硬件平台基于工业级的PC主板，基本操作系统平台是DOS。分组过滤器软件是基于以上平台的一个DOS应用程序。过滤器通过DOS的命令解释器运行后，多线程核心调度模块接管整个系统。内存管理基于DOS的内存块链，实现自身的堆空间管理以最大限度地利用系统内存和克服单任务系统的栈堆检查。文件系统管理也基于DOS的常规文件系统。

图3是分组过滤器对分组的处理过程图。系统流过的IP分组都要通过分组过滤模块的检查才能进入IP路由模块，把分组过滤规则加载到某一个接口上以后，分组过滤模块就根据规则对进入或流出该接口的每个IP分组进行检查，作出通过、拒绝通过、审计等动作。

图4是分组过滤模块的内部结构及其与外部模块间的逻辑关系。

图5是本发明的管理系统体系结构图。管理系统包括管理器、安全控制器(CA)、过滤器代理和它们三者之间用来交换管理信息的FCMP(防火墙控制信息协议)协议。管理系统的主要功能是对过滤器的各项参数作出配置和对过滤器的运行情况进行监视和控制；并且，为了保证过滤器的安全，要对过滤器管理人员的身分进行鉴别，还要对管理系统和运行系统间的通信进行加密传输。

过滤器代理驻留在被管对象分组过滤器上，通过FCMP接收管理器发来的配置命令，由命令解释器/规则编译器执行后将配置参数注入运行系统中，从而控制系统的运行。总的说来，过滤器代理与管理器之间的通信方式为客户机/服务器模式，FCMP协议定义了二者之间的请求(管理器)-应答(过滤器代理)对的格式及同步关系。当过滤器代理监测到系统中发生的一些“敏感”事件时，也会利用FCMP TRAP主动发起请求，通知管理器。

SDLP(简单数据链路协议)协议是一个特地为点对点直连线路(RS-232C)设计的数据链路层协议。

图6是安全控制器(CA)的系统结构框图。本发明本身的安全性是通过CA以及管理信息加密传输实现的。图中的CA Proxy(安全控制器代理)包括两部分，一是代理过滤器，二是代理管理器。代理过滤器接收来自管理器的请求，交代理管理器传给过滤器。代理管理器接收来自过滤器的请求，交代理过滤器传给管理器。

图7是过滤器软件模块及数据流图。过滤器内部运行两大数据流，一是通过RS-232C串行接口、来往于分组过滤器与管理器之间的FCMP请求/应答流(简称FCMP流)，一是进出分组过滤器网络端口的IP分组流。

参与FCMP流的模块有串行端口驱动程序、SDLP模块、加解密模块、FCMP模块、过滤器代理和命令解释模块。过滤器代理是整个FCMP流的中心。它作为一个后台进程(或线索)驻留在系统中，等待来自管理器的FCMP请求，将FCMP请求转换成命令，传给命令解释器；过滤器代理得到命令解释器的执行结果后，将FCMP应答传回管理器。

加解密模块位于FCMP模块和SDLP模块之间，换言之，经SDLP模块和串行端口驱动程序传送的数据都经过加密，而FCMP模块处理的数据均未经加密或已经解密。

过滤器交给命令解释器的命令包括执行命令、配置命令和过滤规则。命令解释器将过滤规则交给过滤规则编译器，编译后放入Startup区的规则表中，供分组过滤模块使用。对于配置命令，命令解释器先进行处理，调用相应函数修改分组过滤器的系统状态，然后将配置命传输采用加密技术，同时对网络内的分组过滤器进行鉴别和认证；系统管理器经由安全控制器与企业内部网连接，实施对本发明系统设备的设置、监视、运行参数(含访问控制表)的配置和控制；读卡器与系统管理器相连，当系统管理器要对防火墙中涉及网络安全控制参数进行配置时，必须向读卡器口插入安全卡，并输入正确的个人识别号码才能进入配置状态。

图8是安全控制器的软件模块及数据流图。CA中运行两个FCMP流，一个是代理过滤器与管理器之间的FCMP流，另一个是代理管理器之间的FCMP流。

CA中的两个FCMP流处理过程与分组过滤器中的FCMP流处理过程大致相同。其中代理管理器是FCMP请求的发起者，而代理过滤器是FCMP请求的接收者。代理管理器与分组过滤器构成客户机/服务器，管理器与代理过滤器构成另一对客户机/服务器。代理管理器与代理过滤器之间的信息交换通过一个全局变量区实现。

CA的另一个重要功能是验证管理员的身份，以允许或拒绝对分组过滤器的访问。图中的认证模块实现上是一个身份证算法，建立在SDLP帧的基础上。CA对数据加密时所用到的加密密钥来自一个存放密钥的内部表。

图9是系统管理器的软件模块与数据流图。FCMP协议堆栈(含FCMP模块、SDLP模块、

串行端口驱动模块)和用户界面是管理器的主要组成部分。其中FCMP协议各模块作为客户端向分组过滤器发送管理员命令，并接收来自分组过滤器的返回结果。由于CA的存在，事实上管理器并不直接跟分组过滤器通信，与管理器通过RS-232C端口直接通信的是CA。管理器FCMP客户的服务器端是CA上的代理过滤器。

管理器的另一重要功能是验证管理人员的身份。合法的管理人员拥有一个表明其身份的IC卡，其中存有管理员的个人识别号码(PIN)。在管理员被允许进入管理器正常操作以前，必须将IC卡插入管理器读卡器中，经IC卡处理模块读入其PIN，然后传到CA上的认证模块进行身份认证。若认证成功，则可进入管理器操作，否则管理器拒绝进入正常操作。

说　明　书　附　图

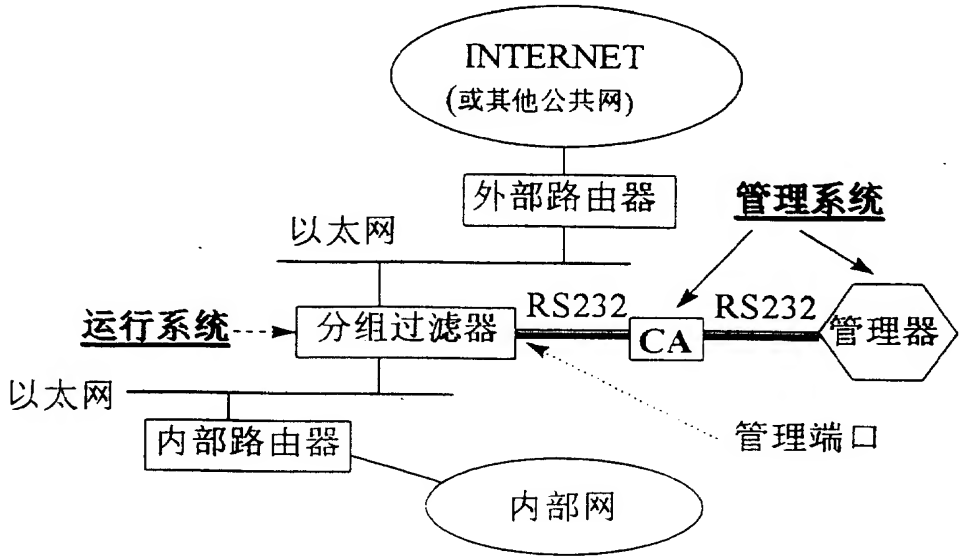


图　1　　体系结构

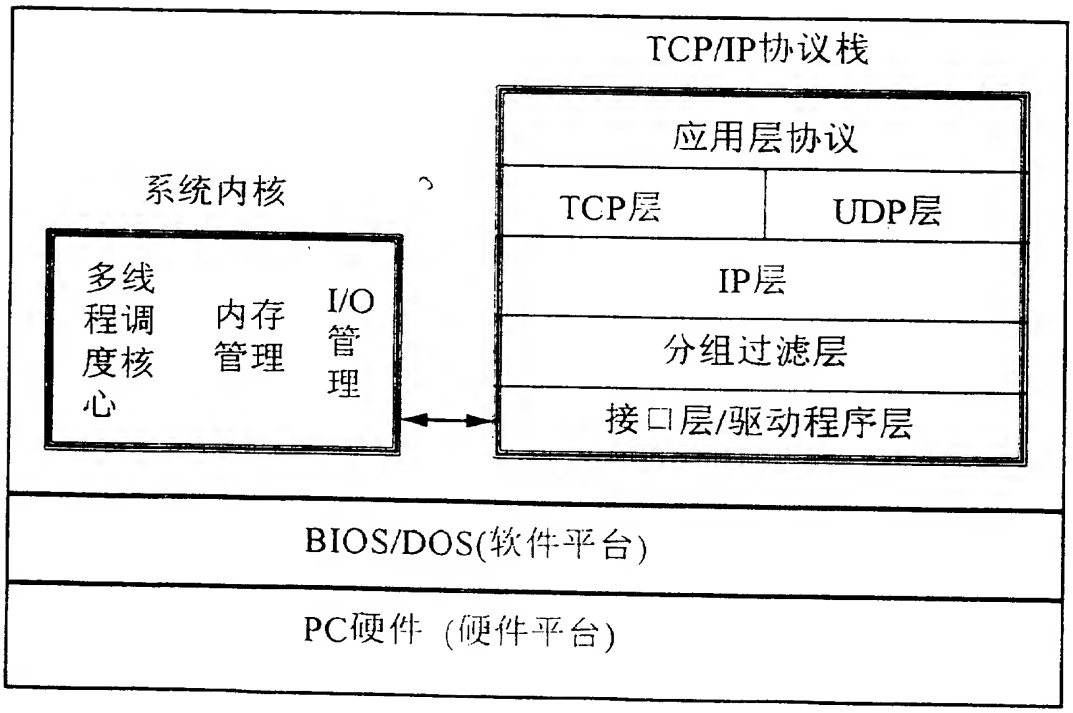


图　2.分组过滤器系统结构

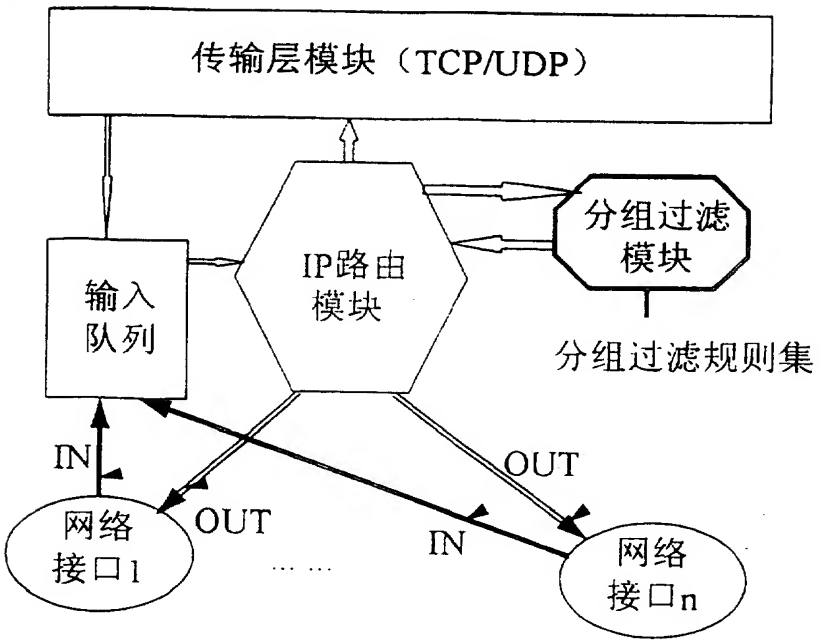


图3 分组过滤器对分组的处理

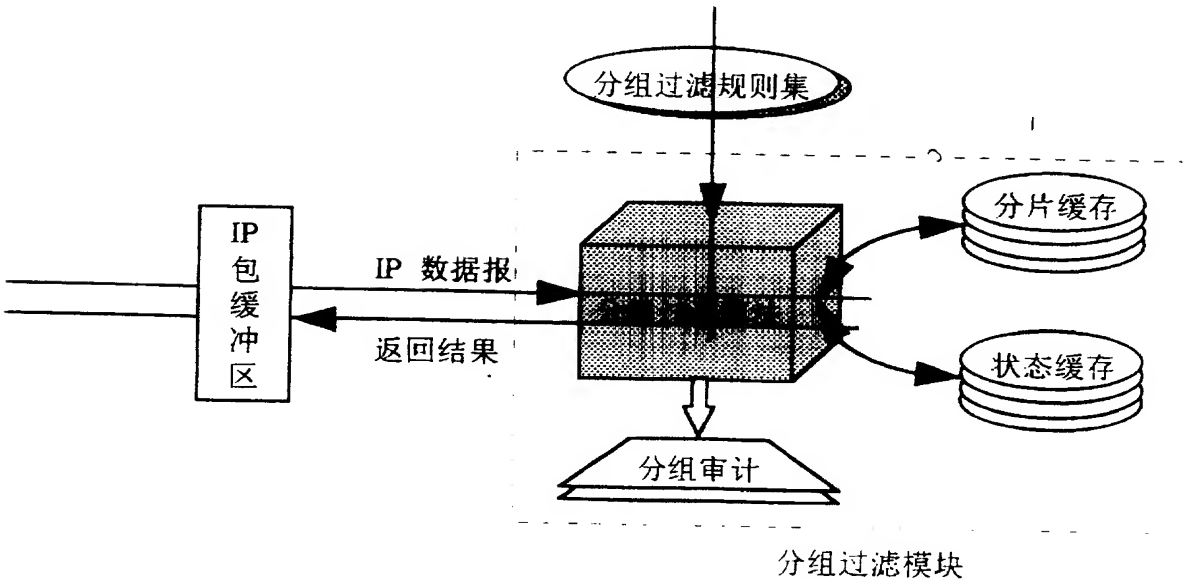


图 4 分组过滤模块的内部结构及其与外部模块间的逻辑关系

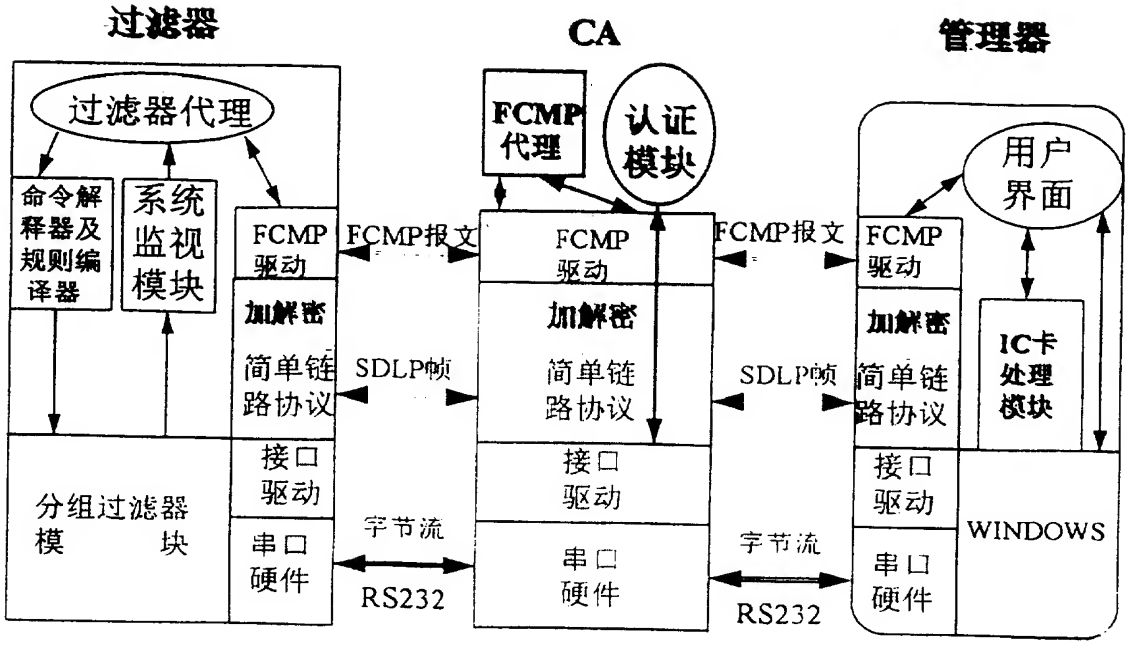


图 5　管理系统体系结构

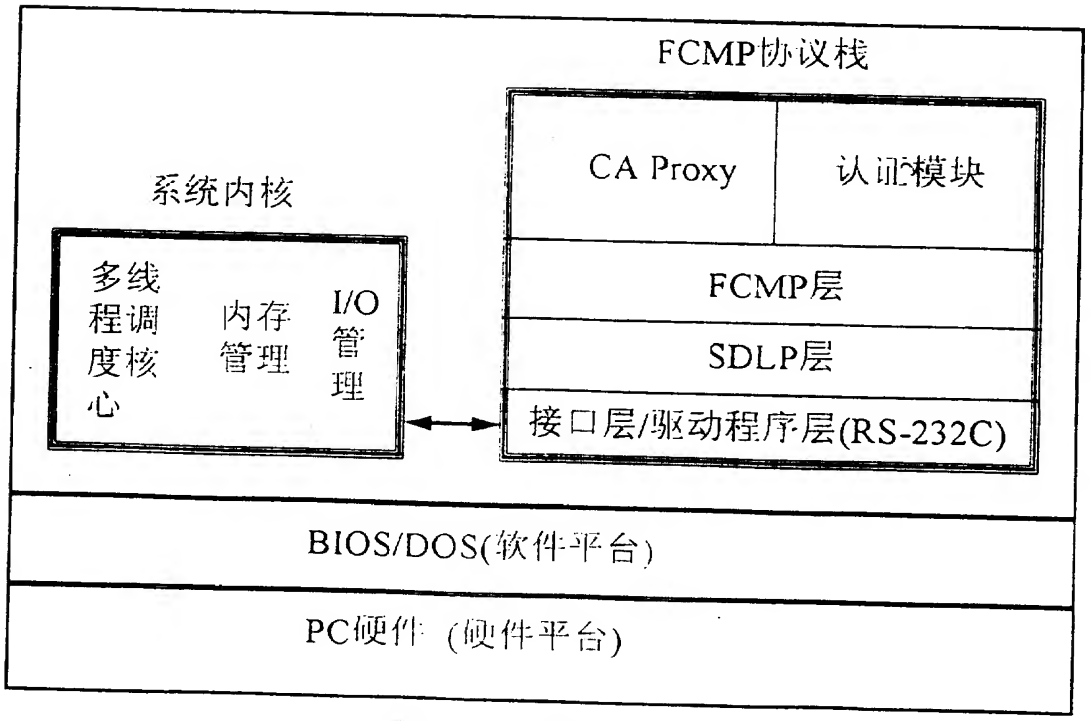


图6　CA系统结构

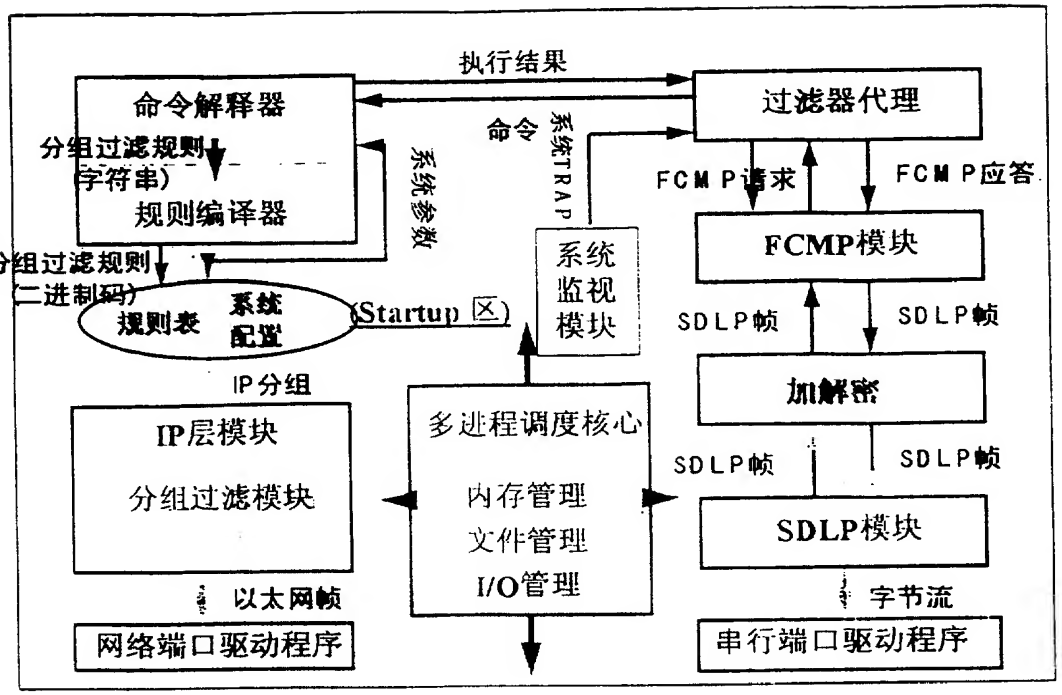


图7　分组过滤器软件模块及数据流

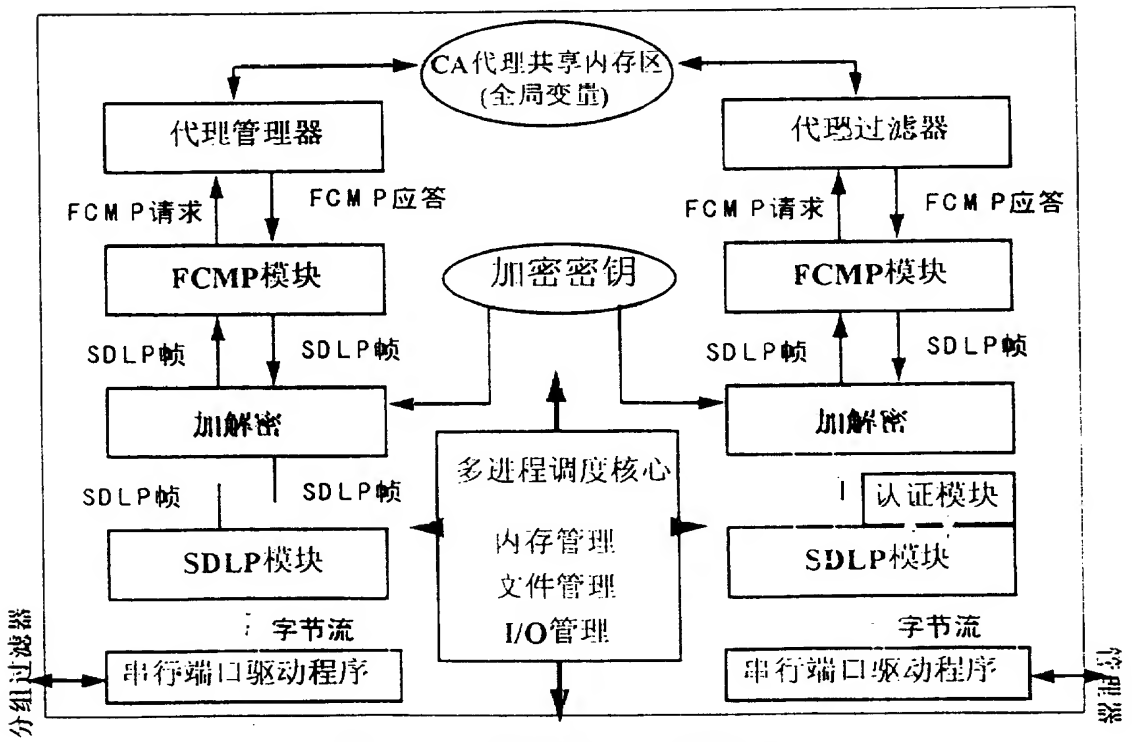


图8　CA软件模块及数据流

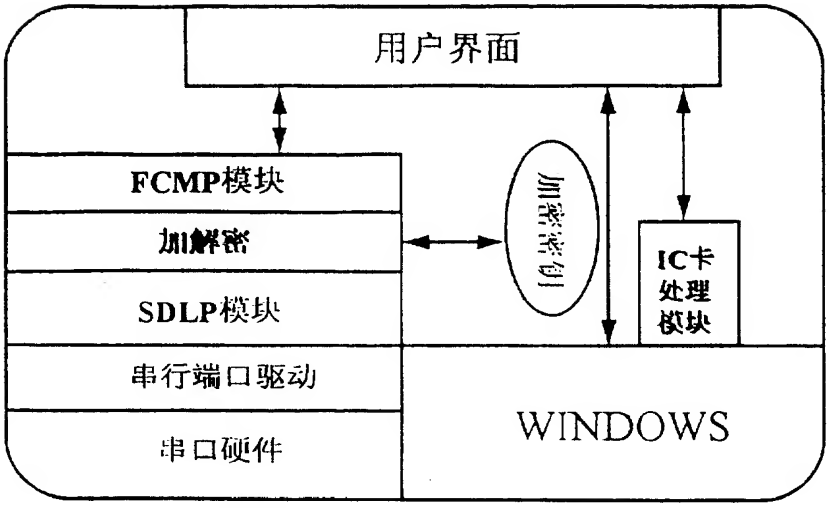


图 9 管理器软件模块与数据流